Information Security Quick Reference Guide - Data Classifications with Research Examples

HARVARD Information Security

CLASSIFICATION				
IRB Determined as Non-Sensitive		IRB-Determined as Sensitive		
L1 = Public Publicly available and unrestricted data	**L2** Unpublished non-sensitive research data, whether identifiable or not. Active research at Harvard is at least L2 until published.	**L3** Some regulated data, or data that could be damaging to the subject's financial standing, career or economic prospects, personal relationships, insurability, reputation, or be stigmatizing	**L4** Data that could place the subject at risk of significant criminal or civil liability or data that require stronger security measures per regulation	**L5** Data that could place the subject at severe risk of harm or data with contractual requirements for exceptional security measures
Examples • Published research data • Data that is publicly available • Non-restricted, publicly available datasets (e.g., Behavioral Risk Factor Surveillance System (BRFSS); NHIS: National Health Interview Survey) as long as the following criteria are met: 1) Research will NOT involve merging any of the data sets in such a way that individuals might be identified; 2) Researcher will NOT enhance the public data set with identifiable, or potentially identifiable data	**Examples** • Self-collected de-identified data, anonymized survey data or aggregate statistics • Self-collected, de-identified biospecimens or genomic data • Other research data that is identifiable but is not considered sensitive • Self-collected non-sensitive survey data, qualitative data such as interviews, or intervention outcome data • Usability data • Non-sensitive audio or video recordings • Non-sensitive observational notes	**Examples** • Education records/student data subject to FERPA • Employment records, employee performance data • Sensitive self-reported health history (US) • Constellation of variables that when merged, become identifiable and/or sensitive • Personal or family financial circumstances (record via surveys or interviews) • Data collection about controversial, stigmatized, embarrassing behaviors (e.g., infidelity, divorce, racist attitudes) • U.S. prisoner administrative data that would not cause criminal or civil liability • Information about U.S. criminal conduct that, if disclosed, could damage the subject's reputation, relationships, or economic prospects[1] • Other information about U.S. criminal conduct that, if disclosed, would not place the subject at risk of significant criminal punishment (see Level 4) • Data sets shared with Harvard under contractual obligation (e.g. corporate NDA, DUA, other contracts at OVPR) at Level 3 controls or with general expectation of confidentiality or data ownership • **Non-US criminal data: PI should consult with Research Compliance or OGC for guidance** • **GDPR data <u>not</u> reaching level of "extra sensitive" –** this includes racial or ethnic origin, political opinions, religious, or philosophical beliefs, trade union membership, sex life or sexual orientation	**Examples** • Government issued identifiers (e.g. Social Security Number, Passport number, driver's license, travel visa, known traveler number) • Individually identifiable financial account information (e.g. bank account, credit or debit card numbers) • HIPAA-regulated PHI (including 18 identifiers)/ HIPAA-regulated Limited Data Set (even if Not Human Subject Research)[2] • Information that, if disclosed, could place the subject at risk of significant criminal punishment (e.g., violent crimes, theft and robbery, homicide, sexual assault, drug trafficking, fraud and financial crimes)[3] • Information that, if disclosed, could put the subject at risk of violent reprisals from the government or other social or political groups • Identifiable U.S. prisoner data that could lead to additional criminal or civil liability • Individually identifiable genetic information that is not Level 5 • Data sets shared with Harvard under contractual obligation at Level 4 controls (whether corporate NDA, DUA, other contracts at OVPR) • **GDPR "extra sensitive" data** – biometric, genetic, or health information.	**Examples** • Data with implications for national security • Certain individually identifiable medical records and genetic information categorized as extremely sensitive. • Data that would put subject's life at risk, if disclosed

GDPR data sensitivity: See https://security.harvard.edu/eu-general-data-protection-regulation-gdpr

[1]ADVISORY NOTE: This could include past crimes for which the subject has served time but that are not matters of public record or are not known to the subject's family, employer, or local community.

[2]Harvard is a hybrid entity, meaning that only certain divisions (HUHS, HSDM Clinic) are HIPAA covered entities. Each Harvard Investigator is required to comply with all applicable privacy and security policies of the HIPAA-covered entity in which that Investigator, as part of a research protocol, is handling PHI or from which the Investigator is drawing PHI. However, data that leaves the covered entity and is transferred to a non-HIPAA covered entity of Harvard is not considered to be HIPAA regulated data.

[3]ADVISORY NOTE: Investigators should consider the criminal laws applicable to the subject. For example, a subject's abortion history could be Level 4 data if she resides in a jurisdiction that criminalizes abortion; and a subject's political activism may expose the subject to prosecution in certain nations. Investigators should also take into account the likelihood of prosecution, considering, among other factors, how much time has passed, the severity of the conduct in question, and the nature and extent of punishment ordinarily imposed in the jurisdiction. Information about conduct that is punishable by civil or even criminal fines, but not imprisonment, often may not merit Level 4 classification.

Revision Date: 08/09/2023

Data Handling Quick Reference Guide

HARVARD Information Security

General Safeguards for all non-public data:

- Share only with those authorized to have access
- Use caution when discussing in public places
- Secure paper-based information in locked desk/office/cabinet when not in use
- Report possible or actual loss immediately to your supervisor or Security Officer

L5 handling and disposal requirements are specific to each project. Consult with Harvard Information Security on all L5 implementations.

Never share passwords/PINS with anyone or carry them with the device they unlock!

HANDLING			
Activity by Data Level	**L2**	**L3**	**L4**
Printing	Do not leave unattended on copiers/printers	Do not leave unattended on copiers/printers	Send to printer using stored/locked job. Enter passcode at machine to print (see security.harvard.edu for instructions).
Mailing paper-based info	Put in a closed mailing envelope/box and send via Interoffice or US mail.	Put in a sealed envelope/box and send via interoffice or US mail.	Put in a sealed envelope/box and send via FedEx/UPS/USPS mail with tracking/delivery confirmation where feasible.
Storing electronic files on work or personal computer (including portable devices)	Computer must meet Harvard security requirements, including device password, anti-virus, current patches, encryption, and remote wiping.	Computer must meet Harvard security requirements, including device password, anti-virus, current patches, encryption, and remote wiping.	Never copy/store L4 data onto your work or personal computer. Data should remain within the secure managed system or encrypted external storage media.
Storing files on external portable storage media	No specific requirements	USB stick, CD/DVD, back-up tape, etc. must be encrypted and password protected.	USB stick, CD/DVD, back-up tape, etc. must be encrypted and password protected.
Sharing files with authorized individuals	Use approved collaboration tools and share with specific individuals, not anonymous or guest links.	Use approved collaboration tools and share with specific individuals, not anonymous or guest links.	Use only security-cleared L4 SharePoint or network locations to share files with named individuals.
Sending data/files to authorized individuals	Use email and send only to those authorized to view it.	Encrypt when transmitting data both internally and externally: Use a School-supported Secure File Transfer method (e.g. OneDrive, Accellion). On website forms, use HTTPS.	Encrypt when transmitting data both internally and externally: Use a School-supported Secure File Transfer method (e.g. L4 SharePoint, Accellion). On website forms, use HTTPS.
Engaging vendors to store/process data	Written contracts are strongly recommended.	Ensure written university contract includes appropriate university security rider(s).	Engage Information Security for a security review and include Harvard's data security addendum in the vendor/hosting agreement.
Deleting electronic files	Use standard Delete/"X" commands and empty trash bin	Use standard Delete/"X" commands and empty trash bin	Use a secure overwrite or removal tool (e.g. Identity Finder)

How to dispose/recycle paper:

L1 Data only for single-stream recycling

L2-L4 Data to be shredded and recycled

How to dispose of devices and/or prepare them for recycling or upgrade:

Enter incorrect passwords until device reformats itself or select Reset in Settings

Shred CD/DVD at provided shredders or contact local IT Support

Contact local IT Support for pick-up or drop-off: they will remove data and recycle

Revision Date: 08/09/2023